

PCT

WELTORGANISATION FÜR GEISTIGES EIGENTUM
Internationales Büro



INTERNATIONALE ANMELDUNG VERÖFFENTLICH NACH DEM VERTRAG ÜBER DIE
INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT)

(51) Internationale Patentklassifikation 7 : G07F 7/08, G07C 9/00, G06K 19/10		A1	(11) Internationale Veröffentlichungsnummer: WO 00/49583 (43) Internationales Veröffentlichungsdatum: 24. August 2000 (24.08.00)
(21) Internationales Aktenzeichen: PCT/EP00/01057		(81) Bestimmungsstaaten: CA, CN, CZ, HU, ID, IL, IN, JP, PL, RU, US, europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).	
(22) Internationales Anmeldedatum: 10. Februar 2000 (10.02.00)		Veröffentlicht <i>Mit internationalem Recherchenbericht.</i>	
(30) Prioritätsdaten: 199 06 388.5 16. Februar 1999 (16.02.99) DE			
(71) Anmelder (<i>für alle Bestimmungsstaaten ausser US</i>): BUNDESDRUCKEREI GMBH [DE/DE]; Oranienstrasse 91, D-10958 Berlin (DE).			
(72) Erfinder; und			
(75) Erfinder/Anmelder (<i>nur für US</i>): FREYTAG, Claus [DE/DE]; Galvanistrasse 8, D-10587 Berlin (DE).			
(74) Anwalt: RIEBLING, Peter; Postfach 31 60, D-88113 Lindau (DE).			
(54) Title: METHOD AND DEVICE FOR THE PERSONALISATION AND VERIFICATION OF IDENTIFICATION AND SECURITY DOCUMENTS AND AN IDENTIFICATION AND SECURITY DOCUMENT WHICH CAN BE USED THEREWITH			
(54) Bezeichnung: VERFAHREN UND VORRICHTUNG ZUR PERSONALISIERUNG UND VERIFIZIERUNG VON IDENTITÄTS- UND SICHERHEITSDOKUMENTEN SOWIE EIN DAMIT VERWENDBARES IDENTITÄTS- UND SICHERHEITSDOKUMENT			
(57) Abstract			
<p>The invention relates to a method and device for personalising and verifying identification and security documents and to a security document (13) which can be used therewith. The identification or security document contains data (15) specific to the individual in alphanumeric and/or graphical form, which is either printed on the document and/or stored in the same. According to the invention, the data (15) specific to the individual and/or correlated data is also present in/on the document in a second form which can be machine-read. This data and the data specific to the individual can be read out of the document and checked for consistency, using an appropriate test control unit (10).</p>			

(57) Zusammenfassung

Die Erfindung betrifft ein Verfahren und eine Vorrichtung zur Personalisierung und Verifizierung von Identitäts- und Sicherheitsdokumenten sowie ein damit verwendbares Sicherheitsdokument (13). Das Identitäts- oder Sicherheitsdokument (13) weist personenbezogene Daten (15) auf, die in alphanumerischer und/oder graphischer Form auf dem Dokument aufgebracht und/oder in dieses eingebracht sind. Erfindungsgemäß sind die personenbezogenen Daten (15) und/oder mit diesen korrelierte Daten in einer zweiten maschinenlesbaren Form auf/in dem Dokument vorhanden und können zusammen mit den personenbezogenen Daten mittels eines entsprechenden Prüfgerätes (10) vom Dokument ausgelesen und auf Übereinstimmung überprüft werden.

LEDIGLICH ZUR INFORMATION

Codes zur Identifizierung von PCT-Vertragsstaaten auf den Kopfbögen der Schriften, die internationale Anmeldungen gemäß dem PCT veröffentlichen.

AL	Albanien	ES	Spanien	LS	Lesotho	SI	Slowenien
AM	Armenien	FI	Finnland	LT	Litauen	SK	Slowakei
AT	Österreich	FR	Frankreich	LU	Luxemburg	SN	Senegal
AU	Australien	GA	Gabun	LV	Lettland	SZ	Swasiland
AZ	Aserbaidschan	GB	Vereinigtes Königreich	MC	Monaco	TD	Tschad
BA	Bosnien-Herzegowina	GE	Georgien	MD	Republik Moldau	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagaskar	TJ	Tadschikistan
BE	Belgien	GN	Guinea	MK	Die ehemalige jugoslawische Republik Mazedonien	TM	Turkmenistan
BF	Burkina Faso	GR	Griechenland	ML	Mali	TR	Türkei
BG	Bulgarien	HU	Ungarn	MN	Mongolei	TT	Trinidad und Tobago
BJ	Benin	IE	Irland	MR	Mauretanien	UA	Ukraine
BR	Brasilien	IL	Israel	MW	Malawi	UG	Uganda
BY	Belarus	IS	Island	MX	Mexiko	US	Vereinigte Staaten von Amerika
CA	Kanada	IT	Italien	NE	Niger	UZ	Usbekistan
CF	Zentralafrikanische Republik	JP	Japan	NL	Niederlande	VN	Vietnam
CG	Kongo	KE	Kenia	NO	Norwegen	YU	Jugoslawien
CH	Schweiz	KG	Kirgisistan	NZ	Neuseeland	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Demokratische Volksrepublik Korea	PL	Polen		
CM	Kamerun	KR	Republik Korea	PT	Portugal		
CN	China	KZ	Kasachstan	RO	Rumänien		
CU	Kuba	LC	St. Lucia	RU	Russische Föderation		
CZ	Tschechische Republik	LI	Liechtenstein	SD	Sudan		
DE	Deutschland	LK	Sri Lanka	SE	Schweden		
DK	Dänemark	LR	Liberia	SG	Singapur		

5 **Verfahren und Vorrichtung zur Personalisierung und Verifizierung von
Identitäts- und Sicherheitsdokumenten sowie ein damit verwendbares
Identitäts- und Sicherheitsdokument**

10 Gegenstand der Erfindung ist ein Verfahren und eine Vorrichtung zur
Personalisierung und Verifizierung von Identitäts- und Sicherheitsdokumenten
sowie ein damit verwendbares Identitäts- und Sicherheitsdokument.

15 Hochsichere Identitätsdokumente wie Ausweise, Passports, Lizenzen,
Führerscheine, Kfz-Scheine, Mitgliedskarten, Betriebs- und Dienstausweise,
Kreditkarten und dergleichen bestehen aus einem unpersonalisierten
Dokumentenkörper auf und/oder in welchem die persönlichen Daten des Inhabers
in vom Dokumentenkörper untrennbarer Weise eingebracht werden. Hierzu sind
mehrere Verfahren bekannt, wobei z.B. fotografische Prozesse, Lasergravur,
Thermotransfer, Dye-Sublimation, xerografische Laserverfahren, Ink-Jet
20 Verfahren etc. zu nennen sind.

25 Die Dokumentenkörper selbst können aus verschiedenen Materialien,
Kombinationen, Konstruktionen von Materialien, Formaten und Zusätzen
bestehen. Beispiele für Materialien sind: Identitäts- und Sicherheitspapiere,
Kunststoffe wie Polycarbonat und Polyvinylchlorid. Beispiele für Formate sind:
ID0, ID1 [ICAO und ISO-Normen, z.B. ISO 7816]

30 Besagte Identitätsdokumente werden aus Sicherheitsgründen in einem
Unternehmen der Wert- und Sicherheitstechnik zentral hergestellt und
personalisiert. Bei der Personalisierung werden die Personaldaten des Inhabers
mit Hilfe verschiedener Verfahren in den Dokumentenkörper eingebracht.

35 Grundsätzlich lassen sich zwei Klassen von Personaldaten unterscheiden:
alphanumerische und grafische Personaldaten. Alphanumerische Personaldaten
bestehen grundsätzlich aus Buchstaben, Ziffern und Sonderzeichen der
verschiedenen Zeichensätze (Fonts). Ein Beispiel für den Umfang eines
Zeichensatzes des europäischen Sprachraums ist in der ISO 8859 dargestellt. Es

- 5 bestehen daneben jedoch weitere Zeichensätze für z. B. arabische oder asiatische Schriften. Eine besondere Ausprägung stellen die OCR-Schriftsätze in den ICAO-Zeilen von Identitätsdokumenten dar, da sie maschinenlesbar sind. Damit ist es möglich, mit Hilfe eines Lesegeräts (Scanner) alphanumerische Daten des Identitätsdokuments auszulesen und zu verifizieren.
- 10 Typische grafische Daten eines Identitätsdokuments sind: Portraits, Unterschriften, Fingerabdrücke, Barcodes, Hoheitszeichen und Logos. Diese Grafikdaten werden mittels moderner fotografischer oder digitaler Druck- und Gravierverfahren in das Identitätsdokument eingebracht. Damit ist gewährleistet, daß die Personaldaten untrennbar mit dem Dokument verbunden sind.
- 15 Für die alphanumerischen Personaldaten sind automatische Verfahren bekannt, die z. B. auf Flughäfen die ICAO-Zeilen mit Hilfe entsprechender Lesegeräte (Scanner) einlesen und mit den Einträgen in einem elektronischen Personenarchiv (Datenbank) vergleichen können. Dieses Verfahren setzt jedoch die Online-
- 20 Verbindung zwischen dem Scanner und einer zentralen Datenbank voraus und läßt sich bisher nicht auf grafische Daten anwenden, da diese eine hohe Komplexität und damit ein hohes Datenvolumen aufweisen. Die hohe Komplexität bedingt eine hohe Prozessorleistung der beteiligten Informationsverarbeitungsanlagen zur Übertragung und Verarbeitung des
- 25 Datenvolumens. Wegen des großen Datenvolumens wird ein hoher Speicherbedarf und eine breitbandige Übertragungsleistung der angeschlossenen Kommunikationseinrichtungen benötigt. Selbst unter Ausnutzung modernster Informationsverarbeitungsanlagen würden hier im praktischen Einsatz unvertretbar lange Verarbeitungs- und Antwortzeiten entstehen.
- 30 Ein weiterer Nachteil des oben geschilderten Verfahrens ist die Notwendigkeit der ständigen Online-Fähigkeit der zentralen Personendatenbank. In der Praxis bedeutet dies, daß ständig komplexe, ausfallsichere und teure Informationsverarbeitungsanlagen verfügbar und betriebsbereit sein müssen, und
- 35 daß beispielsweise einem Polizist in einem Streifenwagen oder in einer örtlichen Wache die genannten notwendigen Prüfmöglichkeiten nicht zur Verfügung stehen.

- 5 Kritisch sind in diesem Zusammenhang auch nationale juristische Restriktionen, z. B. des Personendatenschutzes, die die maschinengestützte Identitätsfeststellung von Personen verbieten, da die Gefahr besteht, daß die Daten ausgewertet und daraus Bewegungsprofile erstellt werden können.
- 10 Aufgabe der Erfindung ist, ein Verfahren und eine Vorrichtung zur Personalisierung und Verifizierung von Sicherheitsdokumenten sowie ein geeignetes Sicherheitsdokument bereitzustellen, welches es erlaubt, die Echtheit insbesondere von grafischen Personaldaten mit verhältnismäßig einfachen Mitteln automatisch verifizieren zu können. In der Praxis bedeutet dies, daß eine
- 15 Authorisierungsperson wie z. B. ein Polizei- oder Grenzkontrollbeamter feststellen können muß, ob z. B. das Portrait eines vorgelegten Identitätsdokuments zu diesem gehört.

Diese Aufgabe wird durch die kennzeichnenden Merkmale der unabhängigen
20 Patentansprüche gelöst.

Die erfindungsgemäße Lösung umfasst im wesentlichen folgende Merkmale und Vorteile:

- 25 - die Verifizierung ist mit verhältnismäßig einfachen Mitteln möglich,
- die Verifizierung findet Offline, d. h. ohne Verbindung zu einer zentralen Datenbank statt,
- die Verifizierung führt zu dem Ergebnis, daß die grafischen Daten des bei der Prüfung vorgelegten Identitätsdokuments echt sind, also zu diesem gehören
30 und
- die Verifizierung verstößt nicht gegen geltende Rechtsbestimmungen.

Der visuelle Vergleich zwischen der Präsentation des Gesichts einer Person und der bildlichen Darstellung z. B. als fotografisches Lichtbild oder in gedruckter Form
35 gilt als die klassische Erkennungsmethode schlechthin. Aus diesem Grund wird die Verfahrenslösung im folgenden beispielhaft für das Portrait als Identifikationsmethode beschrieben. Selbstverständlich gelten die Ausführungen

- 5 in angepaßter Form auch für andere grafische Personaldaten, wie z. B. Fingerabdrücke. In einer weiteren Ausführung sind auch akustische Vergleichsmethoden zur Identitätsfeststellung wie z. B. der menschlichen Stimme anwendbar.
- 10 Bei der Personalisierung von Identitätsdokumenten werden Portraits zunehmend mit Hilfe von digitalen Druckverfahren in einem zentralen Wert- und Sicherheitsdruckbetrieb hergestellt. Diese Methode bietet den Vorteil, daß die Produktion auf Datenverarbeitungsanlagen durchgeführt wird, bei der das Portrait in einem rechnergestützten Format vorliegt (Pixeldaten) und für eine
- 15 Weiterverarbeitung effizient genutzt werden kann. Das Volumen eines Portraits für den Einsatz in Identitätsdokumenten beträgt bei einer akzeptable Reproduktionsqualität etwa 70 bis 100 kBytes. Diese Zahlen sind u.a. abhängig von den geometrischen Abmessungen, der Farbe, der Farbtiefe und vom Kompressionsfaktor.
- 20 Der Lösungsweg geht über die Idee, diese graphischen Daten in der herkömmlichen gedruckten und einer zweiten maschinenlesbaren Form in das Identitätsdokument einzubringen. Damit besteht die Möglichkeit bei einer Identitätsprüfung beide Formen des Portraits miteinander zu vergleichen und bei
- 25 erfolgreichem Vergleich die Echtheit des Dokuments zu bestätigen.
- In einer bevorzugten Ausführungsform ist vorgesehen, die Portraitdaten, d.h. die Vergleichsdaten in einem elektronischen Speicherchip abzulegen. Dieser Chip ist Bestandteil des Identitätsdokuments. Als Ausführungsform können Chipkarten
- 30 nach ISO 7816 oder kontaktlose (Transponder)Karten eingesetzt werden. Weitere Möglichkeiten die Grafikdaten in einer zweiten Form abzuspeichern, bieten Barcodes, insbesondere 2D-Barcodes wie z. B. der PDF 417 der Fa. Symbol.
- Beim Einsatz von Halbleiterspeichern beträgt der beschreibbare Speicherbereich
- 35 von geeigneten Chipkarten mit Prozessorfunktionalität derzeit typisch 16 kByte für kontaktbehaftete Karten. Die o. g. Datenmenge eines Portraits ist um ein Vielfaches größer als der verfügbare Speicherplatz. Damit ist es zur Zeit nicht

- 5 möglich, die Pixeldaten eines Portraits in unkomprimierter Form in einer Chipkarte abzulegen. Abgesehen davon würde die Dauer des Auslesens einer derartigen Datenmenge unakzeptabel lange dauern.
- Der wesentliche Nachteil einer unkomprimierten Speicherung besteht jedoch darin, daß die reinen Pixeldaten einen einfachen Fälschungsangriff ermöglichen,
- 10 da ein Angreifer den Chip eines Identitätsdokumentes mit gefälschten Daten überschreiben könnte. Aus diesem Grund muß die Speicherung der Porträtdaten folgende Bedingungen erfüllen:
- die Speichergröße d.h. der Grad der Kompression der Daten muß in einem optimalen Verhältnis von Qualität und Realisierbarkeit stehen und
 - 15 - die Abspeicherung der grafischen Daten muß in einem unverfälschbaren Format durchgeführt werden.

Um die erste Bedingung zu erfüllen, erfolgt eine entsprechende Aufbereitung der grafischen Daten. Die bei der Produktion des Sicherheitsdokuments vorliegenden

20 Grafikdaten entsprechen einer Pixeldarstellung des Portraits. Mit Hilfe dieses Datenstromes wird die Personalisierungseinrichtung angesteuert, um das Bild auf das Dokument zu drucken. Bei einer automatischen Inspektion muß das Bild von einem Verifizierungsgerät aufgenommen werden. Hierzu lassen sich Scanner oder Kameras mit CCD-Technologie (CCD: Charge Coupled Devices) einsetzen.

25 Das gescannte Bild liefert jedoch stets einen anderen Datenstrom als der zur Personalisierung eingesetzte. Dies liegt u. a. daran, daß die Farbwerte des Portraits nie genau rekonstruiert werden können und daß die ursprüngliche Pixelauflösung aufgrund der geometrischen Toleranzen nie genau genug getroffen werden kann.

30 Aus diesem Grund wird ein Verfahren eingesetzt, welches auf einem biometrischen Verfahren zur Generierung des Datensatzes basiert. Hintergrund ist, daß es bei dem Vergleich zweier Portraits nicht auf die reinen Pixeldaten ankommt, sondern daß bestimmte körperliche Merkmale entscheidend sind. Dies entspricht im übrigen auch der Verfahrensweise, wie ein Polizist das Portrait auf

35 der Karte mit dem Gesicht eines Bürgers vergleicht. Ausgewertet werden Merkmale wie z. B.:

- Abstandsverhältnisse zwischen Augen, Nase, Ohren, Mund ,

- 5 - Größenverhältnisse der Sinnesorgane,
 - Ausprägungen der Kopfform und einzelnen Teilen, etc..

Diese biometrischen Merkmale werden aus den Portraitdaten gewonnen und führen zu einem variablen individuellen Datensatz. Je genauer die biometrischen
10 Merkmale ausgewertet werden, desto umfangreicher wird der Datensatz.
Hersteller solcher Systeme geben eine Größe von 1.000 bis 2.000 Byte an, mit
der das Portrait einer Person eindeutig charakterisiert werden kann. Damit steht
ein Datenformat bzw. eine Datenmenge zur Verfügung, welche optimal den
Forderungen zur Speicherung auf einem Kartenchip genügt. Bei der folgenden
15 Ausführung wird dieser Referenzdatensatz, der die charakteristischen Merkmale
eines Portraits beschreibt, Bio-Datensatz (Bio-ref) genannt.

Um die zweite, oben genannte Bedingung zu erfüllen ist vorgesehen, ein
Verfahren einzusetzen, welches auf der Basis einer asymmetrischen
20 Kryptoverschlüsselung die Unverfälschbarkeit des Bio-Datensatzes garantiert.
Asymmetrische Verschlüsselungsverfahren basieren auf einem Schlüsselpaar mit
einem privaten und einem öffentlichen Schlüssel. Die Verschlüsselung wird mit
dem privaten Schlüssel und die Entschlüsselung mit dem öffentlichen Schlüssel
durchgeführt. Der Hersteller der Identitätsdokumente besitzt den zertifizierten
25 privaten Schlüssel des asymmetrischen Kryptoverfahrens wie z. B. RSA. Eine
wesentliche Voraussetzung ist, daß dieser private Schlüssel unberechtigten
Dritten niemals bekannt wird, da sonst das Gesamtsystem angreifbar wird. Aus
diesem Grund darf der private Schlüssel niemals die Kryptobox des
Produktionssystems des Sicherheitsbetriebes verlassen. Sogar die Generierung
30 dieses Schlüssels findet innerhalb der Kryptobox statt. Eine Schlüssellänge von
1024 Bit wird derzeit als unangreifbar betrachtet.

Der im Produktionssystem aus den Pixeldaten gewonnene Bio-Datensatz wird mit
dem privaten Schlüssel des asymmetrischen Kryptoverfahrens verschlüsselt. Im
35 Ergebnis liegt ein verschlüsselter Bio-Datensatz vor, der aufgrund der
Verfahrensinhärenz nur durch die Kryptobox des Sicherheitsbetriebes generiert
werden kann. Dieser verschlüsselte Bio-Datensatz wird im Speicher des Chips

- 5 des Identitätsdokumentes abgelegt. Die Entschlüsselung des Datensatzes ist möglich unter Zuhilfenahme des öffentlichen Schlüssels. Dieser darf bekannt sein, da sich die asymmetrische Kryptoverfahren dadurch auszeichnen, daß sich im Gegensatz zu den symmetrischen Verfahren aus der Bekanntheit eines Schlüssels der andere nicht ableiten läßt.
- 10 Die Erfindung beschreibt den Einsatz eines asymmetrischen Kryptoverfahrens wie z. B: RSA zum Ver- und Entschlüsseln des biometrischen Datensatzes. Diese Verfahren sind allgemein bekannt. Eine Standardbeschreibung der Verfahren findet sich in "Applied Cryptography" von Bruce Schneier, ISBN 0-471-11709-9.
- 15 Gegenstand der Erfindung ist ebenfalls ein Prüfgerät, welches im Feld die Echtheit eines Identitätsdokumentes insbesondere von grafischen Daten feststellt.

Aus Effizienzgründen kann bei der Datensatzgenerierung ein Hash-Algorithmus (z.B. RIPEMD160) eingesetzt werden, welcher aus dem vorliegenden bis zu 20 kByte grossen Bio-Datensatz einen z.B. 160 Bit grossen Hashwert bildet. Dies bietet den Vorteil, daß für die Speicherung der Daten auf den Sicherheitsdokument sehr wenig Speicherplatz benötigt wird und das Verfahren des Prüfens des Identitätsdokuments in der Praxis schneller durchgeführt werden kann.

25 Nachfolgend wird die Erfindung anhand eines Ausführungsbeispiels unter Bezugnahme auf mehrere Zeichnungsfiguren näher erläutert. Dabei gehen aus den Zeichnungen und der zugehörigen Beschreibung weitere Merkmale und Vorteile der Erfindung hervor.

30 Figur 1 zeigt eine einfache stilistische Darstellung einen Portraits mit einigen eingetragenen biometrischen Merkmalen;

Figur 2 zeigt schematisch den Verfahrensablauf und den Datenfluss bei der
35 Personalisierung und Verifizierung eines Sicherheitsdokuments;

- 5 Figur 3 zeigt einen möglichen Aufbau eines Verifizierungsgeräts mit eingebrachtem Sicherheitsdokument.

In Figur 1 ist ein Portrait dargestellt, in welchem einige körperliche (biometrische) Merkmale eingetragen sind:

- 10 A: Ohrenabstand
B: Augenabstand
C: Mundbreite
D: Augen-Mund-Abstand
E: Nase-Augen-Abstand

15

Natürlich gibt es eine Vielzahl von weiteren Merkmalen, die zur Generierung des Bio-Datensatzes herangezogen werden können, z.B. Form des Kinnbereichs, Form der Nase, Narben, Leberflecke etc.

- 20 In der Biometrie (Lehre von der Vermessung lebender Merkmale) sind verschiedene Verfahren bekannt, die z. B. Gesichtsmerkmale erkennen, zuordnen und vermessen. Im Ergebnis steht ein charakteristischer Datensatz zur Verfügung. Die Qualität des Datensatzes ist von der Verfahrensart und der Menge der Daten abhängig. Diese biometrischen Verfahren sind Stand der Technik und
- 25 deren Arbeitsweise soll hier nicht näher erläutert werden.

- Ein Portrait in CMYK-Farbdarstellung mit Paßbildgröße und einer digitalen Auflösung von 600 dpi benötigt ca. 3,5 Mio. Bytes in unkomprimierter Darstellung. Gängige Verfahren wie TIFF, JPEG, Wavelet oder Fraktale Kompression ermöglichen die Reduktion der o. g. Datenmenge. Allerdings sind sie auch immer mit Qualitätsverlusten der Ausgangsdaten behaftet, die eine eindeutige Erkennbarkeit für ein Verifizierungssystem nicht mehr zulassen.

- 30 Die biometrischen Verfahren lösen das Problem, weil sie lediglich die wesentlichen körperlichen Merkmale betrachten. Beispiel: Soll der Augenabstand in einem Wertebereich von 20 mm mit einer Genauigkeit von 0,1 mm bestimmt werden, so lässt sich das Ergebnis in nur einem Byte angeben. Unter

- 5 Berücksichtigung von z.B. tausend solcher biometrischen Merkmale lässt sich ein Portrait mit einer extrem niedrigen Fehlerwahrscheinlichkeit in nur einem kByte Speicherplatz beschreiben.

Das biometrische Verfahren wird bei der Erfindung an zwei Stellen eingesetzt. Bei
10 der Personalisierung wird mit dem biometrischen Verfahren der Bio-Datensatz (Bio-ref) erzeugt, der verschlüsselt und im Chip-Speicher des ID-Dokuments abgelegt wird. Im Prüfgerät (Verifikationsgerät) wird mit Hilfe des selben biometrischen Verfahrens aus dem gescannten Portrait ein zweiter Bio-Datensatz (Bio-scan) generiert. Ein Vergleich beider Bio-Datensätze ergibt das
15 Verifizierungsergebnis.

Der Datenfluss bei der Personalisierung und bei der Verifizierung des Identitätsdokuments ist in Figur 2 dargestellt.

- 20 Bei der Personalisierung des ID-Dokuments liegt zunächst die Datei 1 mit den Pixelportraitdaten einer Person vor. Diese Daten werden einem geeigneten Biometrischen Verfahren 2 unterzogen, wobei sich ein im Datenumfang stark reduzierter Bio-Datensatz (Bio-ref) ergibt. Dieser Bio-Datensatz wird mit Hilfe eines asymmetrischen Verschlüsselungsverfahrens 3 unter Verwendung eines
25 privaten Schlüssels verschlüsselt und in einem auf den ID-Dokument angeordneten Speicherchip 4 gespeichert.

Bei der Verifizierung wird das ID-Dokument in ein Prüfgerät eingeführt. Das Prüfgerät verfügt über eine optische Leseeinrichtung mittels welcher das bildliche
30 Portrait auf dem ID-Dokument gescannt wird, so daß sich eine Pixelportraitdatei 5 ergibt, die in einem Speicher des Prüfgeräts abgelegt wird. Diese Pixeldatei wird dem selben biometrischen Verfahren 6 unterzogen, wie es bereits bei der Personalisierung des Dokuments verwendet wurde, wobei sich ein biometrischer
35 Datensatz 7 (Bio-scan) ergibt, der ebenfalls im Speicher des Prüfgerätes abgelegt wird. Das Prüfgerät verfügt über eine kontaktabhafte und/oder kontaktlose Auslesevorrichtung, mit welcher die Bio-ref-Daten aus dem Speicherchip des ID-

- 5 Dokuments ausgelesen, entschlüsselt und im Speicher des Prüfgerätes gespeichert werden können.
- Im Prüfgerät liegen nun beide Bio-Datensätze, Bio-ref und Bio-scan, vor, die nun mittels eines Verifizierungsverfahrens 8 von einem im Prüfgerät vorhandenen Mikrocomputers verglichen werden. Dieser Vergleich führt zu einem Ergebnis 9,
- 10 welches dem Benutzer optisch und/oder akustisch angezeigt wird. Stimmen die beiden Bio-Datensätze in hohem Masse überein, so ist die Echtheit des ID-Dokuments bewiesen. Stimmen sie nicht ausreichend überein, so ist von einem gefälschten Dokument auszugehen.
- 15 Figur 3 zeigt einer Ausführungsform des Prüfgeräts 10 mit einem Gehäuse 11 etwa in der Größe einer Videokassette. Das Prüfgerät 10 verfügt an einer schmalen Seite über eine Positionierungseinheit, mit deren Hilfe das Identitätsdokument 13 in eine definierte Lage gebracht werden kann. Dies kann z. B. ein Einschubschlitz 12 oder eine Auflagefläche sein. Die korrekte
- 20 Positionierung kann automatisch durch eine Sensorik erkannt werden, die den Start der Prüfung einleitet. Der Start kann jedoch auch manuell durch die Betätigung eines Tasters ausgelöst werden. Geometrisch gegenüber der zu prüfenden Grafik (hier: Portrait 15) befindet sich eine Aufnahmeeinheit, z. B. ein Scanner 16 oder eine Kamera. Der Mikrochip 14, auf dem die Bio-Referenzdaten
- 25 gespeichert sind, wird über eine Kontaktierungseinheit 17 elektrisch angeschlossen. In einer besonderen Ausführungsform erfolgt der Anschluß kontaktlos über ein elektromagnetisches Antennensystem. Das Prüfgerät 10 verfügt über einen Mikrocomputer 18 an den der Scanner 16 und die Chipkontakte 17 angeschlossen sind. Der Mikrocomputer 18 führt die
- 30 digitalen Prüffunktionen aus und gibt über eine Anzeigeeinheit (nicht dargestellt) das berechnete Prüfergebnis aus.

Die Funktionen laufen wie folgt ab. Nach Positionierung des Identitätsdokuments 13 und der Startauslösung wird das Portrait 15 über den Scanner 16

- 35 aufgenommen und in digitale Signale umgewandelt. Damit liegt das Portrait 15 als Pixeldatei in ähnlicher Form vor, wie es zur Personalisierung des Identitätsdokuments im Sicherheitsbetrieb eingesetzt wurde. Diese Pixeldatei wird

- 5 im Speicher des Mikrocomputers 18 abgelegt. Der Prozessor generiert nach dem gleichen Algorithmus wie bei der Personalisierung aus dieser Pixeldatei einen zweiten Bio-Datensatz (Bio-scan), der auch im Speicher des Mikrocomputers 18 abgelegt wird.
- 10 In einem weiteren Schritt liest der Prozessor den verschlüsselten Bio-Datensatz (Bio-ref) aus dem Chip 14 des Identitätsdokumentes 13 aus und legt ihn im Speicher des Mikrocomputers 18 des Prüfgeräts 10 ab. In diesem Speicher steht aufgrund der Initialisierung des Mikrocomputers 18 der öffentliche Schlüssel des kryptologischen Systems zur Verfügung. Mit Hilfe dieses Schlüssels wird der erste
- 15 Bio-Datensatz (Bio-ref) aus dem Chip 14 entschlüsselt. Damit liegen beide Bio-Datensätze (Bio-ref und Bio-scan) in vergleichbarer Form im Prüfgerät 10 vor und die Verifikation kann durchgeführt werden.

- Wie bereits beschrieben, können die beiden Bio-Datensätze aufgrund der
- 20 Aufnahmetoleranzen des gescannten Portraits 15 nicht absolut identisch sein. Ähnliche Verfahren der biometrischen Verifikation liefern Ergebnisse mit Abweichungsraten im Subpromille-Bereich. Unter der Berücksichtigung eines Schwellwertes aus diesem Bereich werden diese Abweichungen toleriert. Festzuhalten ist, daß die Abweichungsraten deutlich niedriger liegen als
 - 25 beispielsweise bei einem visuellen Vergleich eines Portraits mit einer lebenden Person z. B. durch einen Inspektionsbeamten.

- Das Verifikationsergebnis stellt der Prozessor über eine Ausgabeeinheit an der Oberfläche des Prüfgeräts 10 zur Verfügung. Dies kann im einfachsten Fall eine
- 30 Rot/Grün-Leuchteinheit sein, aber auch die digitale Darstellung des Verifikationsergebnisses z. B. in Prozentangabe der Übereinstimmung der Daten oder auch ein akustisches „OK“-Signal.

- Durch geeignete Auswahl der mechanischen und elektronischen Komponenten
- 35 insbesondere des Mikrocomputers 18 läßt sich der Prüfvorgang auf die Dauer von einigen Sekunden einschränken. Der Aufbau des Prüfgeräts 10 ist so ausgelegt, daß es für einen mobilen Einsatz geeignet ist. Aus diesen Gründen verfügt es

- 5 Über eine Energieversorgung aus Batterien oder nachladbaren Akkus und/oder über einen Anschluß an einen Netzadapter oder das 12-Volt-Versorgungsnetz eines PKW.

5

Zeichnungslegende

- 1 Datei
- 2 Biometrisches Verfahren
- 3 Verschlüsselung
- 10 4 Speicherchip mit Bio-ref Datensatz
- 5 Pixelportraitdaten
- 6 Biometrisches Verfahren
- 7 Biometrischer Datensatz (Bio-scan)
- 8 Vergleich
- 15 9 Ergebnis
- 10 Prüfgerät
- 11 Gehäuse
- 12 Einschubschlitz
- 13 ID-Karte
- 20 14 Mikrochip
- 15 Portrait
- 16 Scanner
- 17 Kontaktiereinheit
- 18 Mikrocomputer

5

Patentansprüche

1. Identitäts- oder Sicherheitsdokument, welches personenbezogene Daten aufweist, die in alphanumerischer und/oder graphischer Form auf dem Dokument aufgebracht und/oder in dieses eingebracht sind,
10 dadurch gekennzeichnet,
daß die personenbezogenen Daten (15) und/oder mit diesen korrelierten Daten in einer zweiten, maschinenlesbarer Form auf/in dem Dokument vorhanden sind, und die in der zweiten, maschinenlesbaren Form vorhandenen Daten nach einem biometrischen Verfahren generierte Daten
15 sind.
2. Identitäts- oder Sicherheitsdokument nach Anspruch 1, dadurch gekennzeichnet, daß die in der zweiten, maschinenlesbaren Form vorhandenen Daten in komprimierter Form vorliegen.
20
3. Identitäts- oder Sicherheitsdokument nach einem der Ansprüche 1 oder 2, dadurch gekennzeichnet, daß die in der zweiten, maschinenlesbaren Form vorhandenen Daten in verschlüsselter Form vorliegen.
25
4. Identitäts- oder Sicherheitsdokument nach einem der Ansprüche 1 bis 3, dadurch gekennzeichnet, daß es ein nichtflüchtiges elektronisches Speichermedium (14) umfasst.
30
5. Identitäts- und Sicherheitsdokument nach Anspruch 4, dadurch gekennzeichnet, daß die in der zweiten, maschinenlesbaren Form vorhandenen Daten in dem elektronischen Speichermedium (14) gespeichert sind.
35
6. Identitäts- oder Sicherheitsdokument nach Anspruch 4 oder 5, dadurch gekennzeichnet, daß das Speichermedium Anschlusskontakte zum Einlesen und/oder Auslesen der darauf gespeicherten Daten aufweist.

- 5 7. Identitäts- oder Sicherheitsdokument nach einem der Ansprüche 4 bis 6,
 dadurch gekennzeichnet, daß das Speichermedium Mittel zum drahtlosen
 Einlesen und/oder Auslesen der darauf gespeicherten Daten aufweist.
- 10 8. Identitäts- oder Sicherheitsdokument nach einem der Ansprüche 1 bis 7,
 dadurch gekennzeichnet, daß die in der zweiten, maschinenlesbaren Form
 vorhanden Daten im Form eines Barcodes auf/in das Dokument eingebracht
 sind.
- 15 9. Verfahren zum Personalisieren eines Identitäts- oder Sicherheitsdokuments,
 bei dem personenbezogene Daten in alphanumerischer und/oder graphischer
 Form auf dem Dokument aufgebracht und/oder in dieses eingebracht werden,
 dadurch gekennzeichnet,
 daß die personenbezogenen Daten und/oder mit diesen korrelierte Daten in
 einer zweiten, maschinenlesbarer Form auf das Dokument aufgebracht
 und/oder in dieses eingebracht werden, und daß die in der zweiten,
 maschinenlesbarer Form vorhandenen Daten mittels eines biometrischen
 Verfahrens aus den personenbezogene Daten generiert werden.
- 20 10. Verfahren nach Anspruch 9, dadurch gekennzeichnet, daß personenbezogene
 Daten in digital verarbeitbarer Form verwendet werden.
- 25 11. Verfahren nach einem der Ansprüche 9 oder 10, dadurch gekennzeichnet,
 daß die in der zweiten, maschinenlesbarer Form vorhanden Daten mittels
 eines asymmetrischen Verschlüsselungsverfahrens verschlüsselt werden.
- 30 12. Verfahren nach einem der Ansprüche 9 bis 11, dadurch gekennzeichnet, daß
 die in der zweiten, maschinenlesbarer Form vorhanden Daten komprimiert
 werden.
- 35 13. Verfahren nach einem der Ansprüche 9 bis 12, dadurch gekennzeichnet, daß
 die in der zweiten, maschinenlesbarer Form vorhanden Daten in einem auf/in

5 dem Dokument vorhandenen nichtflüchtigen elektronischen Speichermedium gespeichert werden.

10 14. Verfahren nach einem der Ansprüche 9 bis 13, dadurch gekennzeichnet, daß die in der zweiten, maschinenlesbarer Form vorhanden Daten als Barcode in/auf dem Dokument abgelegt werden.

15 15. Vorrichtung zum Verifizieren eines Identitäts- oder Sicherheitsdokuments, gekennzeichnet durch:

- ein Positioniermittel (12) zum lagerichtigen Positionieren des Identitäts- und/oder Sicherheitsdokuments (13);
- ein erstes Abtastmittel (16) zum Erfassen von auf dem Identitäts- oder Sicherheitsdokument an-/aufgebrachten personenbezogenen Daten (15);
- ein zweites Abtastmittel (17) zum Erfassen von auf dem Identitäts- oder Sicherheitsdokument vorhandenen Vergleichsdaten;
- Mittel (18) zum Speichern, Aufbereiten und Verarbeiten der erfassten Daten und zur Ausgabe und Anzeige von Ergebnisdaten.
- Mittel (18) zur Aufbereitung der personenbezogenen Daten mittels eines biometrischen Verfahrens.

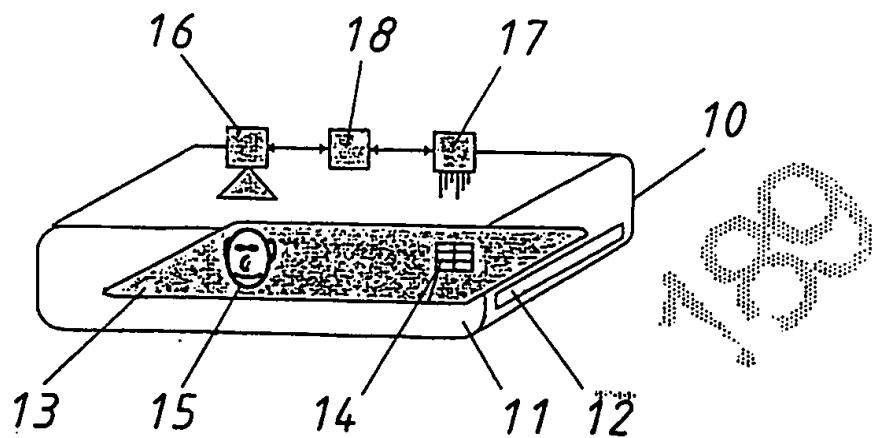
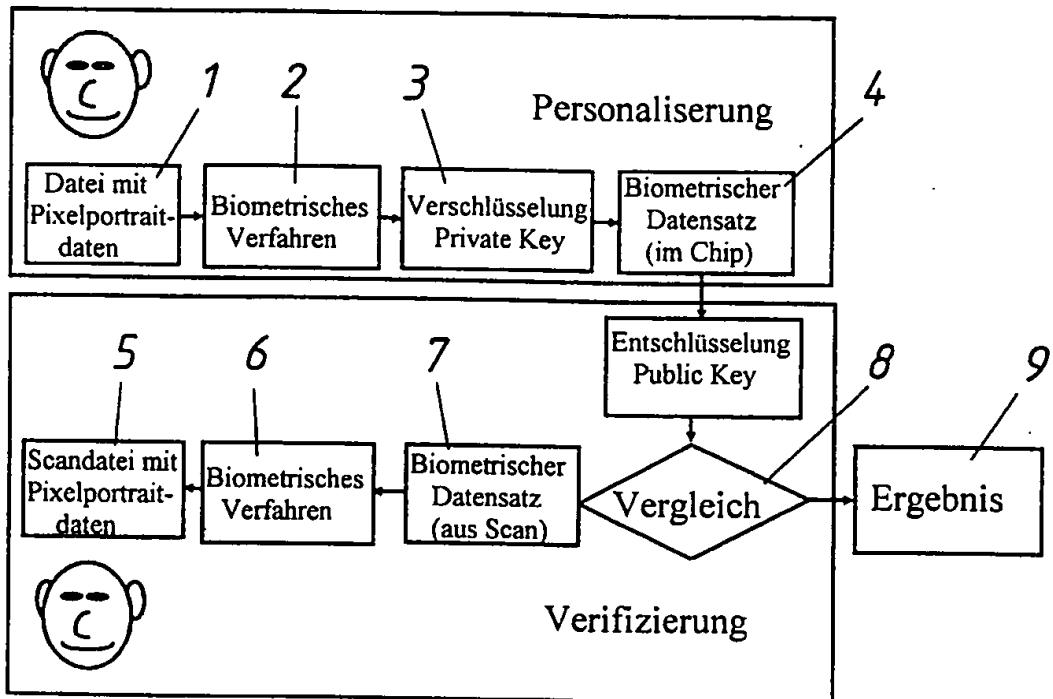
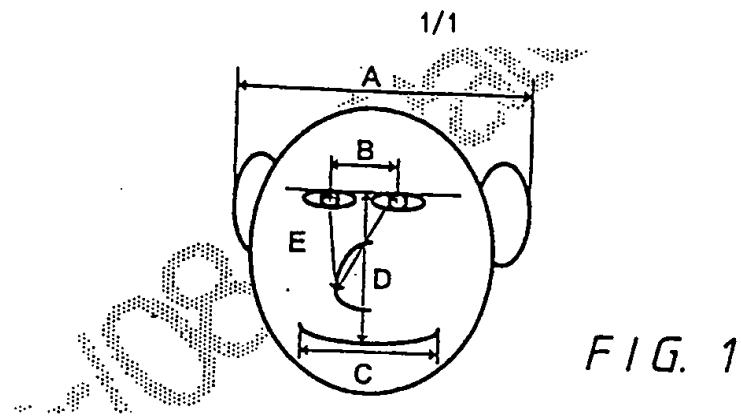
20 25 16. Verfahren zum Verifizieren eines Identitäts- oder Sicherheitsdokuments, welches personenbezogene Daten aufweist, die in alphanumerischer und/oder graphischer Form auf dem Dokument aufgebracht und/oder in dieses eingebracht werden,

gekennzeichnet, durch folgende Schritte:

- Abtasten/Auslesen der personenbezogenen Daten und Speichern dieser Daten in digitaler Form;
- Auslesen von auf dem Dokument abgelegten Vergleichsdaten;
- Vergleichen der personenbezogenen Daten mit den Vergleichsdaten;
- Ausgeben des Ergebnisses des Vergleichs.
- Aufbereitung der personenbezogenen Daten mittels eines biometrischen Verfahrens
- Abspeichern der daraus resultierenden biometrischen Daten

5

17. Verfahren nach Anspruch 16, dadurch gekennzeichnet, daß die biometrischen Daten mit auf/in dem Dokument vorhandenen biometrischen Vergleichsdaten verglichen werden.
- 10 18. Verfahren nach einem der Ansprüche 16 oder 17, dadurch gekennzeichnet, daß die personenbezogenen Daten mittels eines optischen Bildaufnehmers vom Dokument ausgelesen werden.
- 15 19. Verfahren nach einem der Ansprüche 16 bis 18, dadurch gekennzeichnet, daß die in der zweiten, maschinenlesbaren Form vorhanden Daten aus einem auf dem Dokument vorhandenen elektronischen Speichermedium ausgelesen werden.
- 20 20. Verfahren nach einem der Ansprüche 16 bis 19, dadurch gekennzeichnet, daß die in der zweiten, maschinenlesbaren Form vorhanden Daten als Barcode auf dem Dokument vorliegen und mittels eines optischen Bildaufnehmers ausgelesen werden.



INTERNATIONAL SEARCH REPORT

Inten. and Application No
PCT/EP 00/01057

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G07F7/08 G07C9/00 G06K19/10

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G07F G07C G06K

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the International search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	GB 2 289 965 A (CANADA MAJESTY IN RIGHT OF) 6 December 1995 (1995-12-06) page 2, line 35 -page 3, line 33 page 4, line 17 -page 5, line 11 page 8, line 12 - line 36 page 9, line 6 - line 36 figures 1-5	1-14
X	EP 0 805 409 A (I D TEC S L) 5 November 1997 (1997-11-05) column 3, line 27 -column 4, line 5 column 8, line 5 - line 43 figures 1,2	1,8,9,14
Y	— —	2-6, 10-13, 15-20 -/-

Further documents are listed in the continuation of box C.

Patent family members are listed in annex.

* Special categories of cited documents :

- "A" document defining the general state of the art which is not considered to be of particular relevance
- "E" earlier document but published on or after the International filing date
- "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- "O" document referring to an oral disclosure, use, exhibition or other means
- "P" document published prior to the International filing date but later than the priority date claimed

"T" later document published after the International filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"Z" document member of the same patent family

Date of the actual completion of the International search

18 May 2000

Date of mailing of the International search report

25/05/2000

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl.
Fax: (+31-70) 340-3018

Authorized officer

de Ronde, J.

INTERNATIONAL SEARCH REPORT

Intern'l Application No
PCT/EP 00/01057

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5 742 685 A (BERSON WILLIAM ET AL) 21 April 1998 (1998-04-21) column 2, line 12 - line 41 column 3, line 10 -column 4, line 67 figures 1,2 -----	2-6, 10-13, 15-20
A	US 5 131 038 A (CANTARUTTI TRACEY L ET AL) 14 July 1992 (1992-07-14) column 3, line 45 - line 59 figure 1 -----	7

INTERNATIONAL SEARCH REPORT

Information on patent family members

Intern	Application No
PCT/EP 00/01057	

Patent document cited in search report		Publication date		Patent family member(s)		Publication date
GB 2289965	A	06-12-1995		AU 6034994 A		14-09-1994
				DE 4490836 T		11-01-1996
				CA 2115905 A		20-08-1994
				WO 9419770 A		01-09-1994
EP 0805409	A	05-11-1997		ES 2102296 A		16-07-1997
				ES 2105936 A		16-10-1997
				AU 1707795 A		09-10-1995
				CA 2163341 A		28-09-1995
				CN 1128006 A		31-07-1996
				EP 0703094 A		27-03-1996
				ES 2102307 A		16-07-1997
				WO 9525640 A		28-09-1995
				US 5787186 A		28-07-1998
US 5742685	A	21-04-1998		NONE		
US 5131038	A	14-07-1992		NONE		

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP 00/01057

A. KLASIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 7 G07F7/08 G07C9/00 G06K19/10

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierte Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 7 G07F G07C G06K

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der Internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

C. ALS WESENTLICH ANGESEHENDE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	GB 2 289 965 A (CANADA MAJESTY IN RIGHT OF) 6. Dezember 1995 (1995-12-06) Seite 2, Zeile 35 -Seite 3, Zeile 33 Seite 4, Zeile 17 -Seite 5, Zeile 11 Seite 8, Zeile 12 - Zeile 36 Seite 9, Zeile 6 - Zeile 36 Abbildungen 1-5	1-14
X	EP 0 805 409 A (I D TEC S L) 5. November 1997 (1997-11-05) Spalte 3, Zeile 27 -Spalte 4, Zeile 5 Spalte 8, Zeile 5 - Zeile 43 Abbildungen 1,2	1,8,9,14
Y	—	2-6, 10-13, 15-20 —/—

Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

Siehe Anhang Patentfamilie

* Besondere Kategorien von angegebenen Veröffentlichungen:

"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist

"E" älteres Dokument, das jedoch erst am oder nach dem Internationalen Anmeldedatum veröffentlicht worden ist

"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)

"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht

"P" Veröffentlichung, die vor dem Internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist

"T" Spätere Veröffentlichung, die nach dem Internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist

"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erforderlicher Tätigkeit beruhend betrachtet werden

"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erforderlicher Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist

"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der Internationalen Recherche

Anmeldedatum des Internationalen Recherchenberichts

18. Mai 2000

25/05/2000

Name und Postanschrift der Internationalen Recherchenbehörde

Europäisches Patentamt, P.B. 5618 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl.
Fax: (+31-70) 340-3016

Bevollmächtigter Bediensteter

de Ronde, J.

INTERNATIONALER RECHERCHENBERICHT

Intern alle Alterszeichen

PCT/EP 00/01057

C.(Fortsetzung) ALB WESENTLICH ANGEGENANE UNTERLAGEN		
Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
Y	US 5 742 685 A (BERSON WILLIAM ET AL) 21. April 1998 (1998-04-21) Spalte 2, Zeile 12 - Zeile 41 Spalte 3, Zeile 10 - Spalte 4, Zeile 67 Abbildungen 1,2 —	2-6, 10-13, 15-20
A	US 5 131 038 A (CANTARUTTI TRACEY L ET AL) 14. Juli 1992 (1992-07-14) Spalte 3, Zeile 45 - Zeile 59 Abbildung 1 —	7

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Intern: des Aktenzeichen:

PCT/EP 00/01057

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
GB 2289965 A	06-12-1995	AU 6034994 A DE 4490836 T CA 2115905 A WO 9419770 A	14-09-1994 11-01-1996 20-08-1994 01-09-1994
EP 0805409 A	05-11-1997	ES 2102296 A ES 2105936 A AU 1707795 A CA 2163341 A CN 1128006 A EP 0703094 A ES 2102307 A WO 9525640 A US 5787186 A	16-07-1997 16-10-1997 09-10-1995 28-09-1995 31-07-1996 27-03-1996 16-07-1997 28-09-1995 28-07-1998
US 5742685 A	21-04-1998	KEINE	
US 5131038 A	14-07-1992	KEINE	